
Bitdefender
GravityZone
INSTALLATIONSHANDBUCH

Bitdefender GravityZone Installationshandbuch

Veröffentlicht 2015.09.09



Inhaltsverzeichnis

Vorwort

Dieses Handbuch richtet sich an Netzwerkadministratoren, deren Aufgabe es ist, GravityZone in ihrem Unternehmen zu installieren, sowie an Unternehmensadministratoren, die Informationen über die Anforderungen und verfügbaren Sicherheitsmodule von GravityZone benötigen.

In diesem Dokument wird erklärt, wie Sie die GravityZone-Lösung und ihre Sicherheitsagenten auf sämtlichen Arten von Endpunkten in Ihrem Unternehmen installieren und konfigurieren können.

1. Konventionen in diesem Handbuch

Typografie

In diesem Handbuch werden verschiedene Schriftarten verwendet, um die Lektüre zu erleichtern. In der unten stehenden Tabelle erfahren Sie, was welche Schriftart bedeutet.

Erscheinungsbild	Beschreibung
`Beispiel`	Einzugebende Befehle und Syntaxen, Pfade und Dateinamen, Konfigurationen, Dateiausgaben und andere Eingabetexte sind in `nicht-proportionaler` Schrift gedruckt.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Optionen der Benutzeroberfläche, Stichwörter oder Tastenkombinationen werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

1. ÜBER GRAVITYZONE

GravityZone ist eine Sicherheitslösung für Unternehmen, die speziell auf virtuelle und Cloud-Umgebungen zugeschnitten ist. Sie bietet Sicherheitsdienste für physische Endpunkte, virtuelle Maschinen in der Private und der Public Cloud sowie für Exchange-Mail-Server.

GravityZone ist ein umfassendes Produkt mit einer zentralen Verwaltungskonsole, die entweder von Bitdefender in der Cloud gehostet oder als virtuelle Appliance innerhalb des Unternehmens installiert wird. Über diese Konsole können von zentraler Stelle aus Sicherheitsrichtlinien für eine beliebige Zahl an Endpunkten erstellt, zugewiesen und verwaltet werden, unabhängig vom Typ und geographischen Ort dieser Endpunkte.

GravityZone bietet Endpunkten (auch Microsoft-Exchange-Mail-Servern) in mehreren Schichten: Viren- und Malware-Schutz mit Verhaltensanalyse, Schutz vor Zero-Day-Attacken, Anwendungssteuerung und Sandbox, Firewall, Gerätesteuerung, Inhaltssteuerung, Phishing- und Spam-Schutz.

1.1. GravityZone-Sicherheitsdienste

GravityZone enthält die folgenden Sicherheitsdienste:

- Security for Endpoints
- Security for Virtualized Environments
- Security for Exchange

Security for Endpoints

Die Lösung bietet unauffälligen Schutz für Windows-Desktops, -Laptops und -Servern und setzt dabei auf vielfach ausgezeichnete Malware-Schutz-Technologien kombiniert mit einer Zwei-Wege-Firewall, Angriffserkennung, der Steuerung und Filterung des Internet-Zugriffs, dem Schutz von sensiblen Daten sowie Geräte- und Anwendungssteuerung. Geringer Ressourcenverbrauch bringt Leistungsgewinne. Die Lösung bietet viele Vorteile gegenüber herkömmlicher Malware-Schutz-Software, da sie vielfach ausgezeichnete Sicherheitstechnologien mit hoher Benutzerfreundlichkeit und zentraler Verwaltung über das GravityZone Control Center bietet. Proaktive Heuristiken werden eingesetzt, um bösartige Prozesse aufgrund ihres Verhaltens zu erkennen. Dadurch können neue Bedrohungen in Echtzeit erkannt werden.

Security for Virtualized Environments

Security for Virtualized Environments ist die erste umfassende Sicherheitslösung für virtualisierte Rechenzentren zum Schutz von virtualisierten Servern und Arbeitsplatzrechnern auf Windows- und Linux-Systemen. Die Lösung setzt topmoderne Cache-Technologie ein, die gegenüber herkömmlicher Sicherheitssoftware Gewinne in puncto Leistung und Server-Konsolidierung von bis zu 30 % bringt.

Security for Exchange

Bitdefender Security for Exchange bietet Malware-, Spam- und Phishing-Schutz sowie eine Anhang- und Inhaltsfilterung. Die Lösung lässt sich nahtlos mit Microsoft Exchange Server integrieren und schafft so eine Malware-freie E-Mail- und Kollaborations-Umgebung und erhöht damit die Produktivität. Dank mehrfach ausgezeichneter Malware- und Spam-Schutz-Technologie schützt die Software Exchange-Benutzer vor der neuesten und gefährlichsten Malware sowie vor Datendiebstahl.

1.2. GravityZone-Architektur

GravityZone besteht aus den folgenden Komponenten:

- Web-Konsole (Control Center)
- Security Server
- Sicherheitsagenten

1.2.1. Web-Konsole (Control Center)

Bitdefender-Sicherheitslösungen werden innerhalb der GravityZone von einer zentralen Stelle aus verwaltet: dem Control Center. Diese Web-Konsole erleichtert die Verwaltung, indem sie einen Überblick über die gesamte Sicherheitslage des Unternehmens bietet und die Steuerung aller Sicherheitsmodule für virtuelle und physische Arbeitsplatzrechner und Server ermöglicht. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst der größten Unternehmen zu erfüllen.

Das Control Center, eine Web-basiserte Oberfläche, lässt sich mit bestehenden System- und Überwachungssystemen integrieren und macht es so sehr leicht, nicht-verwaltete Arbeitsplatzrechner und Server zu schützen.

1.2.2. Security Server

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Agenten da ist und als Scan-Server fungiert.

Security Server muss auf genügend Hosts installiert sein, um die gewünschte Anzahl an virtuellen Maschinen gewährleisten zu können.

1.2.3. Sicherheitsagenten

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die entsprechenden GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

Bitdefender Endpoint Security Tools

GravityZone schützt physische und virtuelle Maschinen mit Bitdefender Endpoint Security Tools, einem intelligenten Sicherheitsagenten, der sich an die jeweilige Umgebung anpasst und je nach Endpunkttyp automatisch selbst konfiguriert. Bitdefender Endpoint Security Tools kann auf jeder beliebigen Maschine, egal ob virtuell oder physisch, installiert werden und bietet ein flexibles Scan-System. Das macht die Software zur idealen Wahl für gemischte Umgebungen (mit physischen, virtuellen und Cloud-Elementen).

Bitdefender Endpoint Security Tools schützt nicht nur das Dateisystem, sondern auch Microsoft-Exchange-Mail-Server.

Bitdefender Endpoint Security Tools benötigt nur eine einzige Richtlinienvorlage für physische und virtuelle Maschinen und nur ein einziges Installationskit für physische und virtuelle Umgebungen. Bitdefender Endpoint Security Tools ist auch mit physischen Linux-Endpunkten (Arbeitsplatzrechnern und Servern) kompatibel.

Scan-Engines

Die Scan-Engines werden während der Bitdefender Endpoint Security Tools-Paketerstellung automatisch festgelegt. Der Endpunkt-Agent erkennt dabei die Konfiguration der Maschine und passt die Scan-Technologie entsprechend an. Administratoren können die Scan-Engines auch manuell anpassen. Dabei können sie unter den folgenden Optionen wählen:

1. **Lokaler Scan**: für Scans, die auf lokalen Endpunkten durchgeführt werden. Der lokale Scan-Modus eignet sich für leistungsstarke Maschinen, auf denen alle Signaturen und Engines gespeichert sind.
2. **Hybrid-Scan mit leichten Engines (Public Cloud)**: mittlerer Ressourcenverbrauch; gescannt wird in der Cloud und zum Teil auch mithilfe lokaler Signaturen. Dieser Scan-Modus reduziert den Ressourcenverbrauch durch Auslagerung der Scan-Aktivität.
3. **Zentralisierter Scan in der Private Cloud**: geringer Ressourcenverbrauch; benötigt einen Security Server zum Scan. In diesem Fall werden keine Signaturen lokal gespeichert. Die Scan-Aktivität wird auf den Security Server ausgelagert.
4. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Volle Engines)**
5. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (Public Cloud mit leichten Engines)**

* Bei Scans mit zwei Engines wird, wenn die erste Engine nicht verfügbar ist, die Ausweich-Engine verwendet. Der Ressourcenverbrauch und die Netzwerknutzung hängen von der verwendeten Engine ab.

Sicherheitsmodule

Bitdefender Endpoint Security Tools enthält die folgenden Sicherheitsmodule:

- Malware-Schutz
- Active Virus Control
- Firewall
- Inhalts -Steuer.
- Gerätesteuerung
- Power -User

Malware-Schutz

Das Malware-Schutzmodul setzt Signatur-Scans und heuristische Analysen (B-HAVE) ein, um Sicherheit vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und anderen Arten bösartiger Software zu bieten.

Bitdefenders Technologie zur Erkennung von Malware umfasst die folgenden Sicherheitsschichten:

- Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der Signaturdatenbank abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen

spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden, sehr effektiv. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat

- Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt mutmaßliche Malware in einer virtuellen Umgebung aus, um die Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.

Active Virus Control

Für Bedrohungen, die selbst von der heuristische Engine nicht erkannt werden, wurde mit Active Virus Control (AVC) eine dritte Schutzebene eingerichtet.

Active Virus Control überwacht ununterbrochen die laufenden Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel das Verbergen des Prozesstyps, die Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, das Ablegen von Dateien, das Verbergen vor Anwendungen zur Prozessübersicht usw. Jedes verdächtige Verhalten steigert den Verdachtswert des Prozesses. Sobald ein Schwellenwert überschritten wird, wird ein Alarm ausgelöst.



Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Firewall

Die Firewall steuert den Zugriff von Anwendungen auf das Netzwerk sowie auf das Internet. Eine umfangreiche Datenbank enthält eine Liste bekannter, vertrauenswürdiger Anwendungen, denen automatisch Zugriff gewährt wird. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.



Wichtig

Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Inhalts -Steuer.

Mit dem Modul Inhaltssteuerung können Unternehmensrichtlinien für zugelassenen Datenverkehr, Internetzugriff, Datenschutz und Anwendungssteuerung durchgesetzt werden. Administratoren können Scan-Optionen und -Ausschlüsse für den Datenverkehr festlegen, den Internetzugriff auf bestimmte Zeiten beschränken, einzelne Internetkategorien oder URLs blockieren, Identitätsschutzregeln konfigurieren und Rechte für die Verwendung bestimmter Anwendungen festlegen.



Wichtig

Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausnahmen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich wie zum Beispiel USB-Sticks, Bluetooth-Geräte, CD/DVD-Player, Speichermedien und vieles mehr.



Wichtig

Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Power -User

Control-Center-Administratoren können über Richtlinieneinstellungen bestimmten Endpunkt-Benutzern Power-User-Rechte gewähren. Mit dem Power-User-Modul können Benutzern Administratorrechte verliehen werden, mit denen sie über die lokale Konsole Sicherheitseinstellungen anzeigen und verändern können. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.



Wichtig

Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Endpunktrollen

Relais-Rolle

Endpunktagenten mit der Rolle Bitdefender Endpoint Security Tools Relay fungieren als Kommunikations- Proxy- und Update-Server für andere Endpunkte im Netzwerk. Endpunkt-Agenten mit Relais-Rolle werden besonders in Unternehmen mit isolierten Netzwerken benötigt, in denen sämtlicher Datenverkehr über einen einzelnen Zugangspunkt läuft.

In Unternehmen mit großen, geographisch dezentralen Netzwerken reduzieren Relais-Agenten die benötigte Bandbreite, indem sie verhindern, dass geschützte Endpunkte und Security Server eine direkte Verbindung zur GravityZone herstellen.

Nachdem ein Bitdefender Endpoint Security Tools Relay im Netzwerk installiert wurde, können andere Endpunkte per Richtlinie so konfiguriert werden, dass sie über den Relais-Agenten mit dem Control Center kommunizieren.

Bitdefender Endpoint Security Tools Relay-Agenten haben die folgenden Funktionen:

- Alle ungeschützten Endpunkte im Netzwerk finden.

  Diese Funktion ist für die sichere Agenteninstallation in einer GravityZone-Cloud-Umgebung unabdingbar.
- Den Endpunkt-Agenten im lokalen Netzwerk installieren.
- Geschützte Endpunkte im Netzwerk auf dem neuesten Stand halten.
- Die Kommunikation zwischen dem Control Center und verbundenen Endpunkten gewährleisten.
- Als Proxy-Server für geschützte Endpunkte fungieren.
- Optimierung des Netzwerkverkehrs während Updates, Installationen, Scan-Vorgänge und andere ressourcenintensive Aufgaben ausgeführt werden.



Wichtig
Diese Rolle steht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Exchange-Schutz-Rolle

Bitdefender Endpoint Security Tools mit Exchange-Rolle kann auf Microsoft-Exchange-Servern installiert werden, um Exchange-Benutzer vor per E-Mail übertragenen Gefahren zu schützen.

Bitdefender Endpoint Security Tools mit Exchange-Rolle schützt sowohl den Server selbst als auch die Lösung Microsoft Exchange.

Endpoint Security for Mac

Endpoint Security for Mac ist ein leistungsstarker Virenscanner, der sämtliche Arten von Malware aufspüren und entfernen kann: Viren, Spyware, Trojaner, Keylogger, Würmer und Adware. Das Programm ist auf Intel-basierte Macintosh-Arbeitsplatzrechner und -Laptops ausgelegt, auf denen Mac OS X ab Version 10.7 läuft.

Endpoint Security for Mac enthält nur das Malware-Schutz-Modul; die verfügbare Scan-Technologie ist **Lokaler Scan**; alle Signaturen und Engines werden lokal gespeichert.

2. INSTALLATIONSVORAUSSETZUNGEN

Alle GravityZone-Lösungen werden über das Control Center installiert und verwaltet.

2.1. Installationsvoraussetzungen

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren. Dazu benötigen Sie einen Control Center-Benutzer mit Administratorrechten für die Dienste, die Sie installieren möchten, und für die Netzwerk-Endpunkte, die Sie verwalten.

2.1.1. Hardware-Anforderungen

Intel® Pentium kompatibler Prozessor

Betriebssysteme Arbeitsplatzrechner

- 1 GHz oder schneller bei Microsoft Windows XP SP3, Windows XP SP2 64 Bit und Windows 7 Enterprise (32 und 64 Bit)
- 2 GHz oder schneller bei Microsoft Windows Vista SP1 oder neuer (32 und 64 Bit), Microsoft Windows 7 (32 und 64 Bit), Microsoft Windows 7 SP1 (32 und 64 Bit), Windows 8
- 800 MHZ oder schneller bei Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded mit Service Pack 2, Microsoft Windows XP Tablet PC Edition

Betriebssysteme Server

- Minimum: 2,4 GHz Single-Core-CPU
- Empfohlen: 1,86 GHz oder schnellere Intel Xeon Multi-Core-CPU

Freier RAM

Benötigter Arbeitsspeicher bei der Installation (MB)

Betriebssystem	EINZELNE ENGINE					
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
Mac	1024	1024	k.A.	k.A.	k.A.	k.A.

Benötigter Arbeitsspeicher für die tägliche Nutzung (MB)*

Betriebssystem	Virenschutz (einzelne Engine)			Sicherheitsmodule				
	Lokal	Hybrid	Zentrales	Verhalten Scanner	Firewall	Inhalts -Steuer.	Power -User	Update -Server
Windows	75	55	30	+13	+17	+41	+29	+76
Linux	200	180	90	-	-	-	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Festplattenanforderungen

Für die Installation benötigter freier Festplattenspeicher (MB):

Betriebssystem	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1024	1024	400	400	250	250	1024	1024	400	400
Mac	1024	1024	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.



Beachten Sie

- Für Entitäten mit der Rolle Bitdefender Endpoint Security Tools Relay werden mindestens 10 GB zusätzlicher freier Festplattenspeicher benötigt, da dort alle Updates und Installationspakete gespeichert werden.
- Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist.

  Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

  Standardmäßig wird der Agent auf der Systempartition installiert.

Freier Festplattenspeicher für die tägliche Nutzung (MB)*

Betriebssystem	Virenschutz (einzelne Engine)			Sicherheitsmodule				
	Lokal	Hybrid	Zentrales	Verhalten Scanner	Firewall	Inhalts -Steuer.	Power -User	Update -Server
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Bandbreitennutzung

- **Benötigte Bandbreite für Produkt-Updates zwischen dem Endpunkt-Client und dem Update-Server**

  Durch jedes regelmäßige Produkt-Update für Bitdefender Endpoint Security Tools entsteht der folgende Download-Datenverkehr an jedem Endpunkt-Client:

  – Unter Windows: ~20 MB

  – Unter Linux: ~26 MB

- **Benötigte Bandbreite für Signatur-Updates zwischen dem Endpunkt-Client und dem Update-Server**

Update-Server-Typ	Scan-Engine-Typ		
	Lokal	Hybrid	Zentrales
Relais (MB/Tag)	65	58	55
Bitdefender-Update-Server (MB/Tag)	3	3.5	3

- **Für zentralisierte Scans benötigte Bandbreite zwischen dem Endpunkt-Client und dem Security Server**

Gescannte Objekte	Art des Datenverkehrs		Download (MB)	Upload (MB)
Dateien*	Erster Scan		27	841
	Gecachter Scan		13	382
Websites**	Erster Scan	Internet-Datenverkehr	621	N/A
		Security Server	54	1050
	Gecachter Scan	Internet-Datenverkehr	654	N/A
		Security Server	0.2	0.5

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Hybrid-Scan-Datenverkehr zwischen dem Endpunkt-Client und Bitdefender Cloud Services.**

Gescannte Objekte	Art des Datenverkehrs	Download (MB)	Upload (MB)
Dateien*	Erster Scan	1.7	0.6
	Gecachter Scan	0.6	0.3
Internet-Datenverkehr**	Internet-Datenverkehr	650	N/A
	Bitdefender Cloud Services	2.6	2.7

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.



Beachten Sie
Die Netzwerk-Latenz zwischen Endpunkt-Clients und Bitdefender Cloud Server muss unter 1 Sekunde liegen.

- **Signaturherunterlanden-Datenverkehr zwischen den Bitdefender Endpoint Security Tools Relay-Clients und dem Update-Server**

  Clients mit der Bitdefender Endpoint Security Tools Relay laden bei jedem unterstützten Betriebssystem ca. ~16 MB / Tag* vom Update-Server herunter.

  * Verfügbar für Bitdefender Endpoint Security Tools ab Version 6.2.3.569.

- **Datenverkehr zwischen Endpunkt-Clients und dem Control Center**

  Durchschnittlich entsteht pro Tag 618 KB an Datenverkehr zwischen Endpunkt-Clients und dem Control Center.

2.1.2. Unterstützte Betriebssysteme

Windows-Betriebssysteme

Desktop-Betriebssysteme

- Windows 10[(1)]
- Windows 8.1

- Windows 8
- Windows 7
- Windows Vista mit Service Pack 1
- Windows XP mit Service Pack 2 (64-Bit)
- Windows XP mit Service Pack 3

Tablets und eingebettete Betriebssysteme

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded mit Service Pack 2(2)
- Windows XP Tablet PC Edition(2)

Betriebssysteme Server:

- Windows Server 2012/ Windows Server 2012 R2
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003 / Windows Server 2003 R2
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Small Business Server (SBS) 2003
- Windows Home Server

Beachten Sie

(1) Windows 10 wird von Endpoint Security ab Version 5.3.23.704 und von Bitdefender Endpoint Security Tools ab Version 6.2.4.582 unterstützt.

(2) Bestimmte eingebettete Betriebssystemmodule müssen installiert sein, damit Bitdefender Endpoint Security Tools funktioniert.

Linux-Betriebssysteme

- Red Hat Enterprise Linux / CentOS 5.6 oder höher
- Ubuntu 10.04 LTS oder höher
- SUSE Linux Enterprise Server 11 oder neuer
- OpenSUSE 11 oder höher
- Fedora 15 oder höher
- Debian 5.0 oder höher

Zugriff-Scans sind auf allen unterstützten Gast-Betriebssystemen möglich.Auf Linux-Systemen werden Zugriff-Scans in den folgenden Fällen unterstützt:

Kernel-Version	Linux-Distribution	Zugriff-Scan-Unterstützung
2.6.38 oder höher	Alle unterstützt	Die Fanotify-Kernel-Option muss aktiviert sein.
2.6.18 - 2.6.37	Debian 5.0, 6.0 Ubuntu 10.04 LTS CentOS 6.x Red Hat Enterprise Linux 6.x	Hierfür nutzt Bitdefender DazukoFS mit vorgefertigten Kernel-Modulen.

Für andere Distributionen oder Kernel-Versionen müssen Sie das DazukoFS-Modul manuell kompilieren. Informationen zur Vorgehensweise bei der manuellen Kompilierung von DazukoFS finden Sie unter: „Unterstützung von Zugriff-Scans auf virtuellen Linux-Maschinen“ (S. 40).



Beachten Sie

Über Fanotify und DazukoFS können Anwendungen von Drittanbietern den Dateizugriff auf Linux-Systemen steuern. Weitere Informationen finden Sie unter :

- Fanotify-Manpages: http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html.
- Dazuko-Projekt-Website: http://dazuko.dnsalias.org/wiki/index.php/About.

Mac-Betriebssysteme

- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)

- Mac OS X Mavericks (10.9.x)
- Mac OS X Yosemite (10.10.x)

2.1.3. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

2.1.4. Security Server-Anforderungen

Security Server ist eine vorkonfigurierte virtuelle Maschine, die auf einem Ubuntu Server 12.04 LTS (3.2-Kernel) läuft.

Bitdefender Security Server kann auf den folgenden Virtualisierungsplattformen installiert werden:

- VMware vSphere 6.0, 5.5, 5.1, 5.0, 4.1 mit VMware vCenter Server 6.0, 5.5, 5.1, 5.0, 4.1
- vCNS 5.5
- VMware View 5.1, 5.0
- VMware Workstation 8.0.6, 9.x, 10.x, 11.x
- VMware Player 5.x, 6.x, 7.x
- Citrix XenServer 6.2, 6.0, 5.6 oder 5.5 (inkl. Xen Hypervisor)
- Citrix XenDesktop 7.5, 5.5 oder 5.0 (inkl. Xen Hypervisor)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 oder Windows Server 2008 R2, 2012, 2012 R2 (inkl. Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inkl. KVM Hypervisor)
- Oracle VM 3.0



Beachten Sie

Der Support oder Virtualisierungsplattformen kann auf Anfrage bereitgestellt werden.

Speicher- und CPU-Zuteilung für Security Server hängt von der Anzahl und Art der VMs ab, die auf dem Host laufen. In der folgenden Tabelle sind die empfohlenen Ressourcen aufgeführt:

Anzahl geschützter VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

Andere Voraussetzungen:

- Es ist zwar nicht zwingend erforderlich, aber Bitdefender empfiehlt, zur Verbesserung der Leistung Security Server auf jedem physischen Host zu installieren.
- Sie müssen 8 GB Speicherplatz auf jedem Security Server-Host bereitstellen.

2.2. Voraussetzungen für Security for Exchange

Security for Exchange wird via Bitdefender Endpoint Security Tools zur Verfügung gestellt. Die Software schützt sowohl das Dateisystem als auch den Microsoft-Exchange-Mail-Server.

2.2.1. Unterstützte Microsoft-Exchange-Umgebungen

Security for Exchange unterstützt die folgenden Microsoft-Exchange-Versionen und -Rollen:

- Exchange Server 2013 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2010 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle
- Exchange Server 2007 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle

Security for Exchange ist mit Microsoft-Exchange-Datenbankverfügbarkeitsgruppen kompatibel.

2.2.2. Systemanforderungen

Security for Exchange ist mit jedem physischen oder virtuellen 64-Bit-Server (Intel oder AMD) kompatibel, der eine unterstützte Microsoft-Exchange-Server-Version

und -Rolle hat. Weitere Informationen zu Systemvoraussetzungen für Bitdefender Endpoint Security Tools finden Sie unter „Unterstützte Betriebssysteme“ (S. 13).

Empfohlene verfügbare Server-Ressourcen:

- Freier RAM: 1 GB
- Freier Festplattenspeicher: 1 GB

2.2.3. Software-Anforderungen

- Für Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 oder neuer
- Für Microsoft Exchange Server 2013 mit Service Pack 1: KB2938053 von Microsoft.

2.3. GravityZone-Kommunikations-Ports

In der folgenden Tabelle sind die Ports angegeben, die von den GravityZone-Komponenten benutzt werden:

Schnittstelle	Nutzung
80 (HTTP) / 443 (HTTPS)	Port für den Zugriff auf Control Center.
HTTP(s) 80 / 443	Bitdefender-Cloud-Spam-Erkennungsdienst
80	Update Server Port:.
8443 (HTTPS)	Port für die Verbindung der Client/Agend-Software mit dem Kommunikationsserver.
7074 (HTTP)	
7081 / 7083 (SSL)	Ports, die vom Endpunkt-Agenten für die Verbindung zum Security Server verwendet werden.
53 (UDP)	Port für Realtime Blackhole List (RBL)

* Da das Relais ein Update-Server ist, der ununterbrochen auf einem bestimmten Port horchen muss, stellt Bitdefender einen Mechanismus zur Verfügung, mit dem automatisch ein zufälliger Port auf dem eigenen System (127.0.0.1) geöffnet wird, sodass der Update-Server die richtigen Konfigurationsdetails empfangen kann. Dieser Mechanismus greift, wenn der Standard-Port 7074 von einer anderen Anwendung verwendet wird. In diesem Fall versucht der Update-Server, Port 7075 zu öffnen, um auf dem eigenen System zu horchen. Wenn Port 7075 ebenfalls nicht frei ist, sucht der Update-Server nach einem anderen freien Port (im Bereich zwischen 1025 und 65535) über den er am eigenen System horchen kann.

Näheres zu GravityZone-Ports erfahren Sie in diesem Artikel.

3. SCHUTZ INSTALLIEREN

Die folgende Tabelle zeigt die Arten von Endpunkten, die durch die einzelnen Dienste geschützt werden:

Dienst	Endpunkte
Security for Endpoints Security for Virtualized Environments	Physische Computer (Arbeitsplatzrechner, Laptops und Server), auf denen Microsoft Windows, Linux und Mac OS X läuft Virtuelle Maschinen, die auf Microsoft Windows oder Linux laufen
Security for Exchange	Microsoft-Exchange-Server

3.1. Lizenzmanagement

Zur Offline-Registrierung benötigen Sie auch den Offline-Registrierungs-Code, der zum Lizenzschlüssel passt.

Die Sicherheitsdienste in GravityZone erfordern einen gültigen Lizenzschlüssel.

Sie können GravityZone 30 Tage lang kostenlos testen. Während der Testphase stehen alle Funktionen uneingeschränkt zur Verfügung. Sie können den Dienst auf beliebig vielen Computern nutzen. Falls Sie den Dienst weiterhin nutzen möchten, müssen Sie vor Ablauf der Testphase ein kostenpflichtiges Abonnement auswählen und abschließen.

Wenn Sie eine Lizenz erwerben möchten, kontaktieren Sie einen Bitdefender-Händler, oder schreiben Sie uns eine E-Mail an enterprisesales@bitdefender.com.

Ihr Abonnement wird von Bitdefender oder dem Bitdefender-Partner verwaltet, über den Sie den Dienst erworben haben. Manche Bitdefender-Partner sind Sicherheitsdienstleister. Abhängig von Ihrer Abonnementvereinbarung wird der tägliche Betrieb von GravityZone entweder intern von Ihrem Unternehmen oder extern durch den Sicherheitsdienstleister übernommen.

3.1.1. Einen Händler finden

Unsere Händler stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl einer Lizenz-Option, die Ihren Anforderungen gerecht wird.

So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

1. Gehen Sie zur Partnersuche auf der Bitdefender-Website.
2. Wählen Sie Ihr Land, um Informationen zu Bitdefender-Partnern in Ihrer Nähe anzuzeigen.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

3.1.2. Aktivieren einer Lizenz

Beim ersten Abschluss eines kostenpflichtigen Abonnements erhalten Sie einen Lizenzschlüssel. Durch das Aktivieren dieses Lizenzschlüssels aktivieren Sie auch Ihr GravityZone-Abonnement.



Warnung
Die Aktivierung einer Lizenz überträgt deren Umfang NICHT auf die aktuelle Lizenz. Die alte Lizenz wird vielmehr durch die neue überschrieben. Wenn Sie zum Beispiel eine Lizenz für 10 Endpunkte über einer bestehenden Lizenz für 100 Endpunkte aktivieren, erhalten Sie KEIN Lizenzvolumen von 110 Endpunkten. Im Gegenteil, die Anzahl der lizenzierten Endpunkte sinkt von 100 auf 10.

Der Lizenzschlüssel wird Ihnen nach Erwerb per E-Mail zugesendet. Abhängig von Ihrer Dienstleistungsvereinbarung wird Ihr Dienstleister unter Umständen den freigegebenen Lizenzschlüssel für Sie aktivieren. Alternativ können Sie Ihre Lizenz auch manuell aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich über Ihr Konto am Control Center an.
2. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**.
4. Wählen Sie im Bereich **Lizenz** den **Lizenz**-Typ.
5. Geben Sie im Feld **Lizenzschlüssel** Ihren Lizenzschlüssel ein.
6. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
7. Klicken Sie auf **Speichern**.

3.1.3. Aktuelle Lizenzinformationen anzeigen

So zeigen Sie ihre Lizenzinformationen an:

1. Melden Sie mit Ihrer E-Mail-Adresse und dem per E-Mail zugesandten Passwort an der Control Center an.
2. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**. Alternativ können Sie auch auf die **Überprüfen**-Schaltfläche klicken und warten, bis die Control Center die aktuellen Informationen zum vorliegenden Lizenzschlüssel abgerufen hat.

3.2. Die Security Server-Appliance installieren

3.2.1. Security Server auf Hosts installieren

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Clients da ist und als Scan-Server fungiert.

Sie müssen Security Server auf einem oder mehreren Hosts installieren, um die entsprechende Anzahl an virtuellen Maschinen zu schützen.

Dazu müssen Sie die Anzahl der geschützten virtuellen Maschinen sowie die für Security Server auf den Hosts zur Verfügung stehenden Ressourcen und die Netzwerkverbindung zwischen Security Server und den geschützten virtuellen Maschinen bedenken.

Auf virtuellen Maschinen installierte Sicherheitsagenten stellen über TCP/IP eine Verbindung zum Security Server her. Dazu verwenden sie die Informationen, die bei der Installation oder über eine Richtlinie vorgegeben werden.

Lokale Installation

Das Security Server-Paket kann vom Control Center in mehreren verschiedenen Formaten heruntergeladen werden, die mit den gängigsten Virtualisierungsplattformen kompatibel sind.

Installationspakete herunterladen

So laden Sie Installationspakete für Security Server herunter:

1. Gehen Sie zur Seite **Netzwerk > Pakete**.

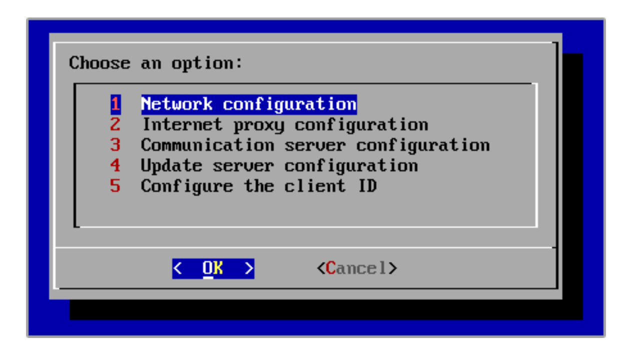
2. Wählen Sie das Security Server-Standardpaket.
3. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Pakettyp aus dem Menü.
4. Speichern Sie das gewählte Paket am gewünschten Speicherort.

Installationspakete installieren

Sobald sie das Installationspaket haben, können Sie es auf dem Host mithilfe eines beliebigen Installationstools für virtuelle Maschinen installieren.

Richten Sie nach der Installation den Security Server wie folgt ein:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu. Alternativ können Sie auch über SSH eine Verbindung zur Appliance herstellen.
2. Melden Sie sich mit den Standardzugangsdaten an.
   - Benutzername: `root`
   - Passwort: `sve`
3. Führen Sie den Befehl `sva-setup` aus. Die Konfigurationsoberfläche der Appliance wird geöffnet.



Security Server-Konfigurationsoberfläche (Hauptmenü)

   Verwenden Sie zur Navigation durch die Menüs und Optionen die `Tabulator`- und Pfeiltasten. Um eine bestimmte Option auszuwählen, drücken Sie `Enter`.

4. Konfigurieren Sie die Netzwerkeinstellungen.

Der Security Server kommuniziert mit den anderen GravityZone-Komponenten über das TCP/IP-Protokoll. Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Gehen Sie dazu wie folgt vor:

a. Wählen Sie im Hauptmenü den Punkt **Netzwerkkonfiguration**.

b. Wählen Sie den Netzwerkadapter aus.

c. Wählen Sie den IP-Adressen-Konfigurationsmodus:

- **DHCP**, wenn Sie möchten, dass der Security Server die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht.
- **Statisch**, wenn kein DHCP-Server vorhanden ist oder wenn im DHCP-Server eine IP-Adresse für die Appliance reserviert wurde. In diesem Fall müssen Sie die Netzwerkeinstellungen manuell konfigurieren.

  i. Geben Sie Hostnamen, IP-Adresse, Netzwerkmaske, Gateway und DNS-Server in die entsprechenden Felder ein.

  ii. Wählen Sie **OK**, um die Änderungen zu speichern.

Beachten Sie
Wenn Sie über einen SSH-Client mit der Appliance verbunden sind, wird Ihre Sitzung sofort beendet, wenn Sie die Netzwerkeinstellungen ändern.

5. Konfigurieren Sie die Proxy-Einstellungen.

   Wenn im Netzwerk ein Proxy-Server verwendet wird, müssen Sie seine Details eingeben, damit der Security Server mit dem GravityZone Control Center kommunizieren kann.



Beachten Sie
Nur Proxy-Server mit Basic Authentication werden unterstützt.

a. Wählen Sie im Hauptmenü den Punkt **Internet-Proxy-Konfiguration**.

b. Geben Sie Hostnamen, Benutzernamen, Passwort und Domaine in die entsprechenden Felder ein.

c. Wählen Sie **OK**, um die Änderungen zu speichern.

6. Konfigurieren Sie die Adresse des Kommunikationsservers.

a. Wählen Sie im Hauptmenü den Punkt **Kommunikationsserverkonfiguration**.

b. Geben Sie die folgende Adresse für den Kommunikationsserver ein:

   `https://cloud-ecs.gravityzone.bitdefender.com:443/hydra`

c. Wählen Sie **OK**, um die Änderungen zu speichern.

7. Konfigurieren Sie die Client-ID.

   a. Wählen Sie aus dem Hauptmenü den Punkt **Client-ID konfigurieren**.

   b. Geben Sie die Unternehmens-ID ein.

      Die ID ist eine Folge von 32 Zeichen, die auf der Seite Unternehmensdetails im Control Center aufgeführt ist.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.

3.3. Installation der Sicherheitssoftware auf Computern und virtuellen Maschinen

Um Ihre physischen und virtuellen Endpunkte zu schützen, müssen Sie auf jedem von ihnen einen Sicherheitsagenten installieren. Der Sicherheitsagent verwaltet den Schutz des lokalen Endpunkts. Zudem kommuniziert er mit dem Control Center, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Weitere Informationen zu verfügbaren Sicherheitsagenten finden Sie unter „Sicherheitsagenten“ (S. 3).

Auf Windows-Maschinen kann der Sicherheitsagent zwei Rollen haben, und Sie können ihn wie folgt installieren:

1. Als einfachen Sicherheitsagenten für Ihre Endpunkte.
2. Als Relais, und somit als Sicherheitsagent und Kommunikations-, Proxy- und Update-Server für andere Endpunkte im Netzwerk.



Warnung

- Der erste Endpunkt, auf dem Sie den Schutz installieren, muss die Relais-Rolle haben, sonst können Sie den Sicherheitsagenten nicht per Fernzugriff auf anderen Endpunkten im selben Netzwerk installieren.
- Der Relais-Endpunkt muss eingeschaltet und online sein, damit die verbundenen Agenten mit dem Control Center kommunizieren können.

Sie können den Sicherheitsagenten auf physischen und virtuellen Endpunkten installieren, indem Sie Installationspakete lokal ausführen oder über Control Center Installationsaufgaben aus der Ferne ausführen.

Es ist wichtig, dass Sie die Anleitung sorgfältig lesen und befolgen, um die Installation richtig vorzubereiten.

Im Normalmodus haben die Sicherheitsagenten eine minimale Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Wenn der Netzwerkadministrator es per Installationspaket und Sicherheitsrichtlinie aktiviert hat, kann der Sicherheitsagent auf Windows-Endpunkten auch im Power-User-Modus ausgeführt werden. In diesem Modus kann der Endpunktbenutzer Sicherheitseinstellungen anzeigen und verändern. Der Control Center-Administrator kann jedoch in jedem Fall festlegen, welche Richtlinieneinstellungen angewendet werden und gegebenenfalls Einstellungen des Power-Users außer Kraft setzen.

Die Sprache der Benutzeroberfläche auf geschützten Endpunkten wird bei der Installation standardmäßig entsprechend der für Ihr Konto eingestellten Sprache festgelegt. Um die Benutzeroberfläche auf bestimmten Endpunkten mit einer anderen Sprache zu installieren, können Sie ein Installationspaket erstellen und die bevorzugte Sprache in den Konfigurationsoptionen dieses Pakets festlegen. Weitere Informationen zur Erstellung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 28).

3.3.1. Vor der Installation

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Endpunkte die Mindestsystemanforderungen erfüllen. Bei manchen Endpunkte kann es notwendig werden, das neueste Service Pack für das Betriebssystem zu installieren oder Speicherplatz zu schaffen. Legen Sie eine Liste der Endpunkte an, die die notwendigen Anforderungen nicht erfüllen, damit Sie diese von der Verwaltung ausschließen können.
2. Entfernen Sie alle bereits installierten Anti-Malware-, Internet-Sicherheits- und Firewall-Lösungen von den Endpunkten (eine Deaktivierung ist nicht ausreichend). Wenn der Sicherheitsagent gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies deren Funktion stören und massive Probleme auf dem System verursachen.

Viele inkompatible Sicherheitsprogramme werden automatisch gefunden und bei der Installation des Sicherheitsagenten entfernt. Weitere Informationen und eine Übersicht über die Sicherheitslösungen, die erkannt werden, erhalten Sie in diesem Artikel in der Wissensdatenbank.



Wichtig

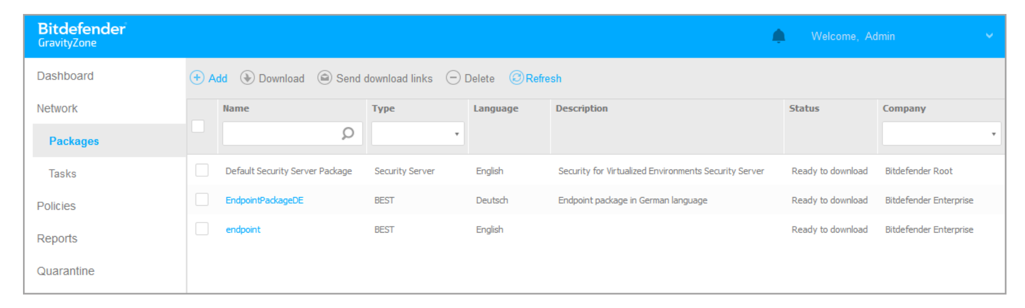
Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Sorgen Sie dafür, dass Sie alle nötigen Zugangsdaten für alle Endpunkte zur Hand haben.
4. Endpunkte müssen eine funktionierende Verbindung zum Control Center haben.

3.3.2. Lokale Installation

Eine Möglichkeit, den Sicherheitsagenten auf einem Endpunkt zu installieren ist es, ein Installationspaket lokal auszuführen.

Sie können die Installationspakete auf der Seite **Netzwerk > Pakete** erstellen und verwalten.



Die Paketübersicht



Warnung

- Die erste Maschine, auf der Sie den Schutz installieren, muss die Relais-Rolle haben, sonst können Sie den Sicherheitsagenten nicht auf anderen Endpunkten im Netzwerk installieren.
- Die Relais-Maschine muss eingeschaltet und online sein, damit die Clients mit dem Control Center kommunizieren können.

Nach der Installation des ersten Clients wird dieser dazu verwendet, um andere Endpunkte über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu finden. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 43).

Gehen Sie zur lokalen Installation des Sicherheitsagenten auf einem Computer folgendermaßen vor:

1. Sie können ein Installationspaket erstellen, das Ihren Anforderungen entspricht.



Beachten Sie
Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

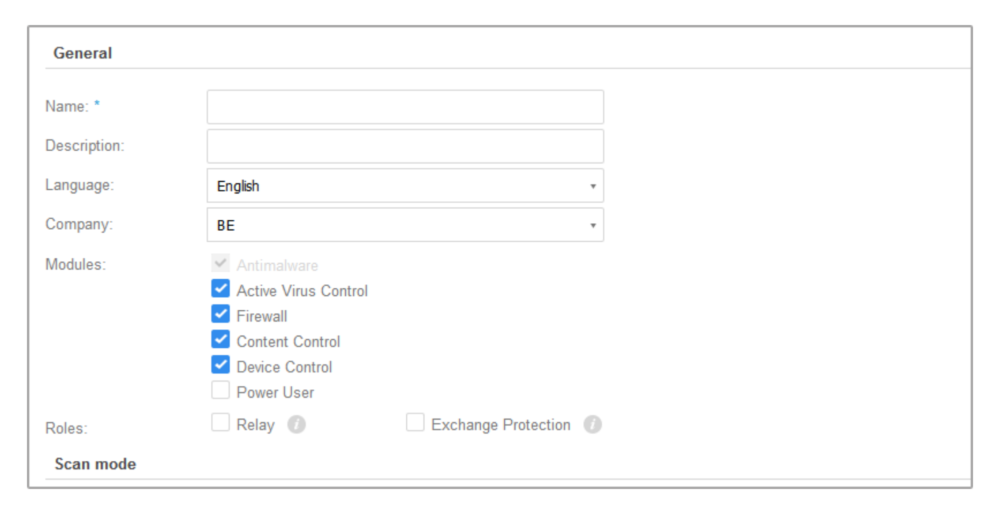
2. Auf diesem Endpunkt müssen Sie zunächst das Installationspaket herunterladen.

   Alternativ können Sie an mehrere Benutzer in Ihrem Netzwerk Download-Links zu den Installationspaketen per E-Mail senden.
3. Im nächsten Schritt Führen Sie das Installationspaket aus.

Installationspakete erstellen

So erstellen Sie ein Installationspaket:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.



Pakete erstellen - Optionen

4. Geben Sie einen aussagekräftigen Namen und eine Beschreibung für das zu erstellende Installationspaket ein.
5. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.
6. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.



Beachten Sie

Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden. Weitere Informationen finden Sie unter „Sicherheitsmodule“ (S. 4).

7. Wählen Sie die Rolle des gewünschten Endpunkts:
   - **Relais**, um das Paket für einen Endpunkt mit der Relais-Rolle zu erstellen. Weitere Informationen finden Sie unter „Relais-Rolle“ (S. 7)
   - **Exchange-Schutz**, um die Sicherheitsmodule für Microsoft-Exchange-Server zu installieren (Malware-Schutz, Spam-Schutz, Inhalts- und Anhangsfilter für den Exchange-E-Mail-Verkehr sowie Bedarf-Malware-Scans in Exchange-Datenbanken). Weitere Informationen finden Sie unter „Security for Exchange“ (S. 2).

8. **Scan-Modus**. Wählen Sie die Scan-Technologie, die am besten zu Ihrer Netzwerkumgebung und den Ressourcen Ihrer Endpunkte passt. Den Scan-Modus können Sie festlegen, indem Sie eine der folgenden Optionen wählen:
   - **Automatisch**. In diesem Fall erkennt der Sicherheitsagent automatisch die Konfiguration der entsprechenden Endpunkte und passt die Scan-Technologie daran an:
     – Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für physische Computer mit geringer Hardware-Leistung.
     – Lokaler Scan (mit vollen Engines) für physische Computer mit hoher Hardware-Leistung.
     – Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für virtuelle Maschinen. In diesem Fall muss mindestens ein Security Server im Netzwerk installiert sein.
     – Zentralisierter Scan in der Private Cloud (Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für EC2-Instanzen. In diesem Fall stellen die EC2-Instanzen automatisch eine Verbindung zum Bitdefender-Security Server her, der in der entsprechenden AWS-Region gehostet ist.

     Beachten Sie
     Es wird empfohlen, die Standard-Scan-Modi für EC2-Instanzen zu verwenden, da diese speziell auf geringen Ressourcenverbrauch ausgelegt sind.

   - **Benutzerdef.**. In diesem Fall können Sie für physische und virtuelle Maschinen verschiedene Scan-Technologien festlegen:
     – Zentralisierter Scan in der Private Cloud (mit Security Server)
     – Hybrid-Scan (mit leichten Engines)
     – Lokaler Scan (mit vollen Engines)
     – Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (mit leichten Engines)

- Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (mit vollen Engines)

* Bei Scans mit zwei Engines wird, wenn die erste Engine nicht verfügbar ist, die Ausweich-Engine verwendet. Der Ressourcenverbrauch und die Netzwerknutzung hängen von der verwendeten Engine ab.

Weitere Informationen zu verfügbaren Scan-Technologien finden Sie hier:„Scan-Engines“ (S. 3)

9. Wenn Sie die Scan-Engines auf Private Cloud (Security Server) stellen, müssen Sie die lokal installierten Security-Server, die Sie verwenden möchten, auswählen und ihre Priorität im Bereich **Security Server-Zuweisung** konfigurieren:
   - Klicken Sie auf die Liste der Security Server in der Tabellenüberschrift. Die Liste der gefundenen Security-Server wird angezeigt.
   - Wählen Sie eine Entität.
   - Klicken Sie in der Spaltenüberschrift **Aktionen** auf die Schaltfläche ⊕ **Hinzufügen**.

     Der Security Server wird der Liste hinzugefügt.
   - Wiederholen Sie diese Schritte, wenn Sie mehrere Security-Server hinzufügen möchten, falls es mehrere gibt. In diesem Fall können Sie ihre Priorität konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile (⌃ und ⌄) klicken. Wenn der erste Security Server nicht verfügbar ist, wird der nächste verwendet, und dann der nächste, usw.
   - Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⊗ **Löschen** am oberen Rand der Tabelle.

   Sie können die Verbindung zum Security Server mit der Option **SSL verwenden** verschlüsseln.
10. Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Maschinen sauber sind, bevor Sie den Client auf ihnen installieren. Es wird dann ein Cloud-Schnell-Scan auf den Maschinen ausgeführt, bevor die Installation gestartet wird.
11. Auf Windows-Endpunkten wird Bitdefender Endpoint Security Tools im Standard-Installationsverzeichnis installiert. Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie Bitdefender Endpoint Security Tools in einem anderen Ordner installieren möchten. Geben Sie in diesem Fall den gewünschten Pfad in das entsprechende Feld ein. Verwenden Sie dabei

Windows-Konventionen (zum Beispiel `D:\Ordner`). Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.

12. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen. Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
13. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.
    - **Bitdefender Cloud**, wenn Sie die Clients direkt aus dem Internet aktualisieren wollen.

      In diesem Fall können Sie auch die Proxy-Einstellungen definieren, wenn die Endpunkte ihre Internetverbindung über einen Proxy-Server herstellen. Wählen Sie **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in die entsprechenden Felder ein.
    - **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

      Wichtig

      Port 7074 muss offen sein, damit die Installation über einen Bitdefender Endpoint Security Tools Relay funktioniert.
14. Klicken Sie auf **Speichern**.



Beachten Sie

Die in einem Installationspaket konfigurierten Einstellungen werden sofort nach der Installation auf den jeweiligen Endpunkt angewendet. Sobald eine Richtlinie auf den Client angewendet wird, werden die Einstellungen dieser Richtlinie durchgesetzt und ersetzen gegebenenfalls die Einstellungen des Installationspakets (z. B. Kommunikationsserver oder Proxy-Einstellungen).

Installationspakete herunterladen

So laden Sie die Installationspakete der Sicherheitsagenten herunter:

1. Melden Sie sich über den Endpunkt, auf dem Sie die Software installieren möchten, am Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Installationspaket aus, das Sie herunterladen möchten.
4. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Installer-Typ aus, den Sie verwenden möchten. Es gibt zwei Arten von Installationsdateien:
   - **Downloader**. Der Downloader lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.
   - **Installationspaket**. Die vollständigen Installationskits sind größer und sie müssen auf einem bestimmten Betriebssystem ausgeführt werden.

     Das vollständige Kit ist dafür da, um den Schutz auf Endpunkten mit einer langsamen bzw. keiner Internet-Verbindung zu installieren. Laden Sie diese Datei auf einen mit dem Internet verbundenen Endpunkt herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe, um die Datei an andere Endpunkte weiterzugeben.



Beachten Sie

Verfügbare Installationspaket-Versionen:

- **Windows OS:** 32-Bit- und 64-Bit-Systeme
- **Linux OS:** 32-Bit- und 64-Bit-Systeme
- **Mac OS X:** nur 64-Bit-Systeme

Vergewissern Sie sich, dass Sie die zum jeweiligen System passende Version wählen.

5. Speichern Sie die Datei auf dem Endpunkt.



Warnung

Die Downloader-Datei darf nicht umbenannt werden, da sonst die Installationsdateien nicht vom Bitdefender-Server heruntergeladen werden können.

Download-Links zu den Installationspaketen per E-Mail senden

Vielleicht möchten Sie andere Benutzer schnell darüber informieren, dass ein Installationspaket zum Download bereitsteht. Gehen Sie dazu wie folgt vor:

1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das gewünschte Installationspaket.
3. Klicken Sie auf die Schaltfläche **Download-Links senden** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adressen aller Benutzer ein, die den Download-Link zum Installationspaket erhalten sollen. Drücken Sie nach jeder E-Mail-Adresse die `Eingabetaste`.

   Vergewissern Sie sich, dass alle eingegebenen E-Mail-Adressen gültig sind.
5. Wenn Sie die Download-Links anzeigen möchten, bevor Sie sie per E-Mail versenden, klicken Sie auf die Schaltfläche **Installationslinks**.
6. Klicken Sie auf **Senden**. An jede eingegebene E-Mail-Adresse wird eine E-Mail mit dem Download-Link gesendet.

Installationspakete ausführen

Damit die Installation erfolgreich durchgeführt werden kann, muss das Installationspaket mit Administratorrechten ausgeführt werden.

Je nach Betriebssystem gestaltet sich die Installation des Pakets etwas unterschiedlich:

- Unter Windows und Mac:
  1. Laden Sie die Installationsdatei vom Control Center auf den gewünschten Endpunkt herunter oder kopieren Sie sie von einer Netzwerkfreigabe.
  2. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
  3. Führen Sie die ausführbare Datei aus.
  4. Folgen Sie den Instruktionen auf dem Bildschirm.
- Unter Linux:
  1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.

2. Laden Sie die Installationsdatei auf den gewünschten Endpunkt herunter oder kopieren Sie sie dorthin.
3. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
4. Verschaffen Sie sich Root-Rechte, indem Sie den Befehl `sudo su` ausführen.
5. Verändern Sie die Rechte für die Installationsdatei, damit Sie sie ausführen können:

```
# chmod +x installer
```

6. Führen Sie die Installationsdatei aus:

```
# ./installer
```

7. Um zu überprüfen, ob der Agent auf dem Endpunkt installiert wurde, können Sie diesen Befehl ausführen:

```
$ service bd status
```

Einige Minuten nachdem der Sicherheitsagent installiert wurde, wird der Endpunkt im Control Center (**Netzwerk**-Seite) als verwaltet angezeigt.

3.3.3. Remote-Installation

Mit Control Center können Sie den Sicherheitsagenten über Installationsaufgaben aus der Ferne auf Endpunkten installieren, die im Netzwerk gefunden wurden.

Nachdem Sie den ersten Client mit Relais-Rolle lokal installiert haben, kann es einige Minuten dauern, bis die anderen Netzwerk-Endpunkte im Control Center angezeigt werden. Von hier an können Sie den Sicherheitsagenten per Fernzugriff auf Endpunkten, die Sie verwalten, mithilfe der Installationsaufgaben im Control Center installieren.

Bitdefender Endpoint Security Tools verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem andere Endpunkte im gleichen Netzwerk gefunden werden können. Gefundene Endpunkte werden als **Nicht verwaltet** auf der **Netzwerk**-Seite angezeigt.

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Endpunkt im Netzwerk installiert haben. Dieser Endpunkt wird dann verwendet, um das Netzwerk zu scannen und Bitdefender Endpoint Security Tools auf den noch nicht geschützten Endpunkten zu installieren.

Anforderungen für die Ferninstallation

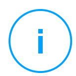
Damit die Ferninstallation funktioniert, müssen die folgenden Punkte gegeben sein:

- Bitdefender Endpoint Security Tools Relay muss in Ihrem Netzwerk installiert sein.
- Jeder Endpunkt, auf dem die Installation erfolgen soll, muss wie im Folgenden beschrieben Fernverbindungen zulassen:
  - Unter Windows: Die administrative Freigabe `admin$` muss aktiviert sein. Konfigurieren Sie jeden Zielarbeitsplatzrechner für die erweiterte Freigabe von Dateien.
  - Unter Linux: SSH muss aktiviert sein.
  - Unter Mac: Fernanmeldung muss aktiviert sein.
- Schalten Sie vorübergehend die Benutzerkontensteuerung auf allen Endpunkten mit Windows-Betriebsystemen, die diese Sicherheitsfunktion beinhalten (Windows Vista, Windows 7, Windows Server 2008 etc.), aus. Wenn die Endpunkte Teil einer Domain sind, können Sie die Benutzerkontensteuerung aus der Ferne über eine Gruppenrichtlinie ausschalten.
- Deaktivieren oder beenden Sie etwaige Firewalls auf den Endpunkten. Wenn die Endpunkt Teil einer Domain sind, können Sie die Windows-Firewall aus der Ferne über eine Gruppenrichtlinie ausschalten.

Ausführen von Ferninstallationsaufgaben

So führen Sie eine Ferninstallationsaufgabe aus:

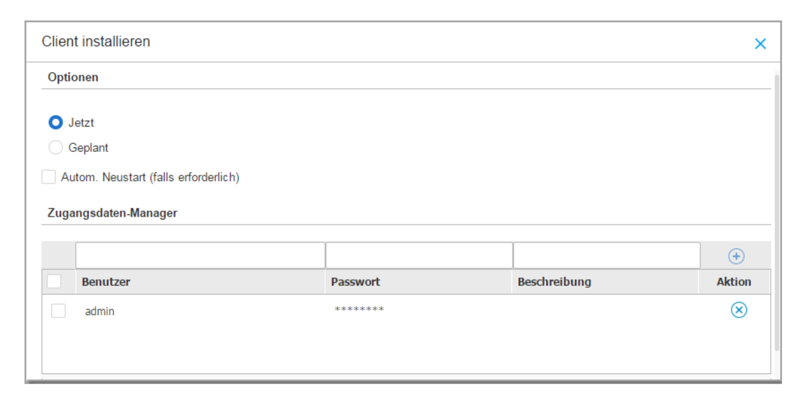
1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.



Beachten Sie
Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Endpunkte anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

4. Wählen Sie die Entitäten (Endpunkte oder Gruppen von Endpunkten) aus, auf denen Sie den Schutz installieren möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Installieren**.

   Der Assistent **Client installieren** wird angezeigt.



Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

6. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:
   - **Jetzt** - hiermit startet die Installation sofort.
   - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.



Beachten Sie
Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden

Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

7. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
8. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.



Wichtig

Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in diesem Artikel.

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

a. Geben Sie im entsprechenden Feld in der Spaltenüberschrift den Benutzernamen und das Passwort eines Administratorkontos ein.

   Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `user@domain.com` oder `domain\user`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`user@domain.com` und `domain\user`).

   Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

b. Klicken Sie auf den Button ⊕**Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.



Beachten Sie

Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben werden müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren.



Wichtig
Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

9. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.



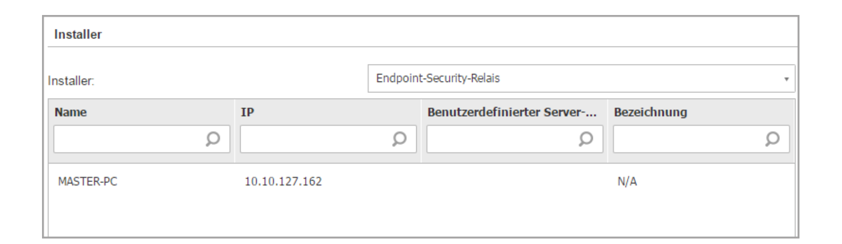
Beachten Sie
Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation des Sicherheitsagenten auf Endpunkten nicht ausgelassen werden.

10. Konfigurieren Sie im Bereich **Installer** das Relais, zu dem die Endpunkte eine Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren:

- Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der Tabelle im Bereich **Installer** aufgeführt. Jeder neue Client muss mit mindestens einem Relais-Client desselben Netzwerks verbunden sein, der als Kommunikations- und Update-Server fungiert. Wählen Sie das Relais, das Sie mit den gewünschten Endpunkten verknüpfen möchten. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.



Wichtig
Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.



- Wenn die gewünschten Endpunkte über einen Proxy mit dem Relais-Agenten kommunizieren, müssen Sie auch die Proxy-Einstellungen definieren. Wählen

Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.

11. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.
12. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

    Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Änderung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 28).

    Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.
13. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

3.3.4. Unterstützung von Zugriff-Scans auf virtuellen Linux-Maschinen

Die Linux-Version von Bitdefender Endpoint Security Tools enthält die Möglichkeit Zugriff-Scans durchzuführen. Dies funktioniert auf bestimmten Linux-Distributionen und Kernel-Versionen. Bitte lesen Sie die Systemanforderungen, um zu erfahren, ob Zugriff-Scans auf Ihrer/Ihren Linux-Maschine(n) möglich sind. Im nächsten Schritt lernen Sie, wie man das DazukoFS-Modul manuell kompiliert.

Kompilieren Sie das DazukoFS-Modul manuell

Gehen Sie wie unten beschrieben vor, um DazukoFS für die Kernel-Version des Systems zu kompilieren und laden Sie danach das Modul:

1. Laden Sie die geeigneten Kernel-Header herunter.
    - Führen Sie auf **Ubuntu**-Systemen den folgenden Befehl aus:

    ```
    $ sudo apt-get install linux-headers-'uname -r'
    ```

- Führen Sie auf **RHEL/CentOS**-Systemen den folgenden Befehl aus:

  ```
  $ sudo yum install kernel-devel kernel-headers
  ```

2. Auf **Ubuntu**-Systemen benötigen Sie das Paket `build-essential`:

   ```
   $ sudo apt-get install build-essential
   ```

3. Kopieren und extrahieren Sie den DazukoFS-Quellcode in einem Verzeichnis Ihrer Wahl:

   ```
   # mkdir temp
          # cd temp
          # cp /opt/BitDefender/share/src/dazukofs-source.tar.gz
          # tar -xzvf dazukofs-source.tar.gz
          # cd dazukofs-3.1.4
   ```

4. Kompilieren Sie das Modul:

   ```
   # make
   ```

5. Installieren und laden Sie das Modul:

   ```
   # make dazukofs_install
   ```

Voraussetzungen für Zugriff-Scans mit DazukoFS

Damit DazukoFS und Zugriff-Scans zusammen funktionieren, müssen die folgenden Voraussetzungen erfüllt sein. Vergewissern Sie sich das die folgenden Punkte auf Ihr Linux-System zutreffen und befolgen Sie die Anweisungen, um Probleme zu vermeiden.

- Die SELinux-Richtlinie muss deaktiviert oder auf **tolerant** gestellt sein. Sie können die Einstellungen der SELinux-Richtlinie einsehen und anpassen, indem Sie die Datei `/etc/selinux/config` bearbeiten.

- Bitdefender Endpoint Security Tools ist ausschließlich mit der Version von DazukoFS kompatibel, die im Installationspaket enthalten ist. Wenn DazukoFS auf Ihrem System bereits installiert ist, muss es vor der Installation von Bitdefender Endpoint Security Tools entfernt werden.
- DazukoFS unterstützt bestimmte Kernel-Versionen. Wenn das in Bitdefender Endpoint Security Tools enthaltene DazukoFS-Paket nicht mit der Kernel-Version des Systems kompatibel ist, kann das Modul nicht geladen werden. Ist das der Fall, können Sie den Kernel auf die unterstützte Version aktualisieren oder das DazukoFS-Modul für Ihre Kernel-Version rekompilieren. Das DazukoFS-Paket befindet sich im Installationsverzeichnis von Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Wenn Sie für Dateifreigaben dedizierte Server wie NFS, UNFSv3 oder Samba verwenden, müssen Sie die Dienste in der folgenden Reihenfolge starten:
  1. Aktivieren Sie im Control Center Zugriff-Scans per Richtlinie.

     Weitere Informationen hierzu finden Sie im GravityZone-Administratorhandbuch.
  2. Starten Sie den Dienst für die Netzwerkfreigabe.

     Für NFS:

     ```
     # service nfs start
     ```

     Für UNFSv3:

     ```
     # service unfs3 start
     ```

     Für Samba:

     ```
     # service smbd start
     ```



Wichtig

Beim NFS-Dienst ist DazukoFS nur mit dem NFS-User-Server kompatibel.

3.3.5. Wie die Netzwerkerkennung funktioniert

Security for Endpoints verfügt über einen automatischen Netzwerkerkennungsmechanismus zur Erkennung von Arbeitsgruppen-Computern.

Security for Endpoints nutzt den **Microsoft-Computersuchdienst** für die Netzwerkerkennung. Der Computersuchdienst ist eine Netzwerktechnologie, die auf Windows-basierten Computern zum Einsatz kommt, um immer aktuelle Listen von Domänen, Arbeitsgruppen und den Computern darin zu verwalten und diese Listen bei Bedarf an Client-Computer weiterzugeben. Computer, die über den Computersuchdienst im Netzwerk erkannt wurden, können durch Eingabe des **Net View**-Befehls im Eingabeaufforderungsfenster angezeigt werden.



Der Net-View-Befehl

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Computer im Netzwerk installiert haben. Von diesem Computer aus wird das Netzwerk gescannt.



Wichtig

Control Center bezieht keine Netzwerkinformationen über Active Directory oder über die Netzwerkübersichtsfunktion in Windows Vista und höher. Die Netzwerkübersicht nutzt eine andere Technologie zur Netzwerkerkennung: das Link-Layer-Topology-Discovery-Protokoll (LLTD).

Control Center übernimmt keine aktive Rolle bei der Ausführung des Computersuchdienstes. Bitdefender Endpoint Security Tools fragt beim Computersuchdienst lediglich die Liste der aktuell im Netzwerk sichtbaren Arbeitsplatzrechner und Server ab (die Suchliste) und leitet diese dann an das Control Center weiter. Das Control Center verarbeitet die Suchliste und fügt neu erkannte Computer zur der Liste der **nicht verwalteten Computer** hinzu. Bereits erkannte Computer werden nach einer Netzwerkerkennungsabfrage nicht gelöscht,

daher müssen Computer, die sich nicht mehr länger im Netzwerk befinden, manuell ausgeschlossen und gelöscht werden.

Die erste Abfrage der Suchliste wird vom ersten im Netzwerk installierten Bitdefender Endpoint Security Tools durchgeführt.

- Falls Bitdefender Endpoint Security Tools auf einem Arbeitsgruppen-Computer installiert wurde, werden im Control Center nur die Computer dieser Arbeitsgruppe angezeigt.
- Falls Bitdefender Endpoint Security Tools auf einem Domänen-Computer installiert wurde, werden im Control Center nur die Computer dieser Domäne angezeigt. Computer aus anderen Domänen können erkannt werden, wenn eine Vertrauensstellung mit der Domäne besteht, in der Bitdefender Endpoint Security Tools installiert ist.

Nachfolgende Netzwerkerkennungsabfragen werden danach stündlich wiederholt. Bei jeder neuen Abfrage teilt das Control Center die verwalteten Computer in Sichtbarkeitsbereiche auf und bestimmt in jedem Bereich einen Bitdefender Endpoint Security Tools zur Durchführung der Aufgabe. Ein Sichtbarkeitsbereich ist eine Gruppe von Computern, die sich gegenseitig erkennen. Normalerweise wird ein Sichtbarkeitsbereich anhand einer Arbeitsgruppe oder Domäne definiert, im Einzelfall hängt dies jedoch von der Netzwerktopologie und Konfiguration ab. Unter Umständen besteht ein Sichtbarkeitsbereich auch aus mehreren Domänen oder Arbeitsgruppen.

Falls ein ausgewähltes Bitdefender Endpoint Security Tools die Abfrage nicht durchführt, wartet Control Center auf die nächste geplante Abfrage, ohne ein anderes Bitdefender Endpoint Security Tools für einen weiteren Versuch auszuwählen.

Um das gesamte Netzwerk sichtbar zu machen, muss Bitdefender Endpoint Security Tools auf mindestens einem Computer in jeder Arbeitsgruppe oder Domäne in Ihrem Netzwerk installiert sein. Im Idealfall sollte Bitdefender Endpoint Security Tools auf mindestens einem Computer in jedem Subnetzwerk installiert sein.

Weitere Informationen zum Microsoft-Computersuchdienst

Der Computersuchdienst auf einen Blick:

- Funktioniert unabhängig von Active Directory.
- Läuft ausschließlich über IPv4-Netzwerken und funktioniert unabhängig innerhalb der Grenzen einer LAN-Gruppe (Arbeitsgruppe oder Domäne). Eine Suchliste wird für jede LAN-Gruppe erstellt und verwaltet.

- Nutzt für die Kommunikation zwischen den Knoten üblicherweise verbindungslose Server-Übertragungen.
- Nutzt NetBIOS über TCP/IP (NetBT).
- Benötigt NetBIOS-Namensauflösung. Es wird empfohlen im Netzwerk eine Windows-Internet-Name-Service-Infrastruktur (WINS) zu unterhalten.
- Ist standardmäßig nicht in Windows Server 2008 und 2008 R2 aktiviert.

Weitere Informationen zum Computersuchdienst finden Sie in der Computer Browser Service Technical Reference im Microsoft Technet.

Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über das Control Center verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein. Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein. Die lokale Firewall muss NetBT-Verkehr zulassen.
- Die Freigabe von Dateien muss auf den Computern aktiviert sein. Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.
- Für Windows Vista und höher muss die Netzwerkerkennung aktiviert werden (**Systemsteuerung > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktion aktivieren zu können, müssen zunächst die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost

- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Bitdefender Endpoint Security Tools den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.



Beachten Sie

Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.

3.4. Schutz auf Exchange-Servern installieren

Security for Exchange integriert sich automatisch mit den Excchange-Servern je nach Server-Rolle. Für jede Rolle werden entsprechend der folgenden Übersicht nur die kompatiblen Funktionen installiert:

	Microsoft Exchange 2013		Microsoft Exchange 2010/2007		
Bestandteile	**Edge**	**Postfach**	**Edge**	**Hub**	**Postfach**
Transport-Ebene					
Antimalware Filtering	x	x	x	x	
Antispam Filtering	x	x	x	x	
Content Filtering	x	x	x	x	
Attachment Filtering	x	x	x	x	
Exchange-Informationsspeicher					
On-demand antimalware scanning		x			x

3.4.1. Vor der Installation

Bevor Sie Security for Exchange installieren, sollten Sie sich vergewissern, dass alle Voraussetzungen erfüllt sind, da sonst eventuell Bitdefender Endpoint Security Tools ohne das Exchange-Schutz-Modul installiert wird.

Damit das Exchange-Schutz-Modul möglichst reibungslos läuft und etwaige Konflikte und unerwünschte Ergebnisse vermieden werden, sollten Sie andere Malware-Schutz- und E-Mail-Filter-Agenten deinstallieren.

Bitdefender Endpoint Security Tools findet und entfernt die meisten Malware-Schutz-Produkte automatisch und deaktiviert auch den eingebauten Malware-Schutz-Agenten von Exchange Server 2013. Eine Liste aller automatisch gefundenen und entfernten Sicherheitssoftware finden Sie in diesem Artikel.

Den eingebauten Exchange-Malware-Schutz-Agenten können Sie jederzeit manuell wieder aktivieren. Dies wird jedoch nicht empfohlen.

3.4.2. Schutz auf Exchange-Servern installieren

Um Ihre Exchange-Server zu schützen, müssen Sie Bitdefender Endpoint Security Tools mit der Exchange-Schutz-Rolle auf jedem dieser Server installieren.

Dazu haben Sie verschiedene Möglichkeiten:

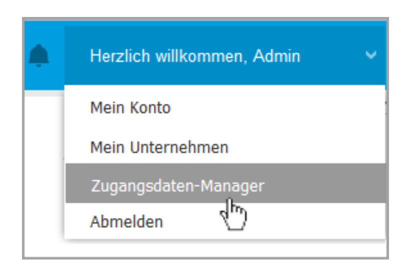
- Lokale Installation durch Herunterladen und Ausführen des Installationspakets auf dem jeweiligen Server.
- Ferninstallation durch Ausführen der Aufgabe **Installieren**.
- Per Fernzugriff durch Ausführen der Aufgabe **Client neu konfigurieren**, falls Bitdefender Endpoint Security Tools bereits das Dateisystem auf dem Server schützt.

Weitere Details zur Installation finden Sie unter „Installation der Sicherheitssoftware auf Computern und virtuellen Maschinen“ (S. 25).

3.5. Zugangsdaten-Manager

Im Zugangsdaten-Manager können Sie die Zugangsdaten, die Sie für die Fernauthentifizierung unter den verschiedenen Betriebssystemen in Ihrem Netzwerk benötigen, definieren.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.

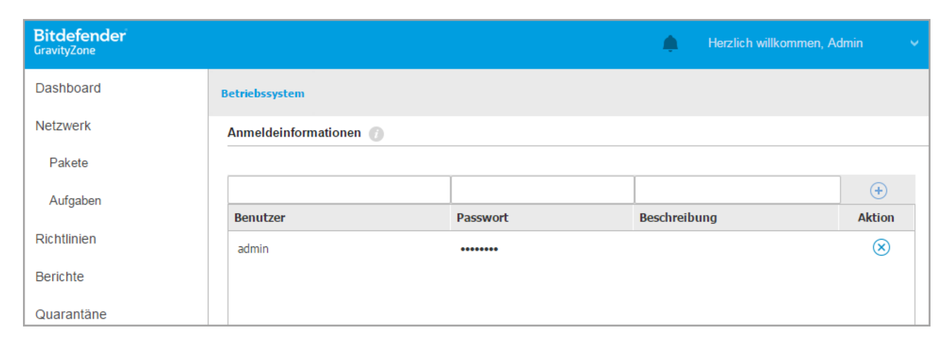


Das Zugangsdaten-Manager-Menü

3.5.1. Zugangsdaten zum Zugangsdaten-Manager hinzufügen

Mit dem Zugangsdaten-Manager können Sie die Administrator-Zugangsdaten verwalten, die für die Fernauthentifizierung während der Ausführung von Installationsaufgaben auf Computern und virtuellen Maschinen in Ihrem Netzwerk nötig sind.

So fügen Sie Zugangsdaten hinzu:



Zugangsdaten-Manager

1. Geben Sie in die entsprechenden Felder im oberen Bereich der Tabelle den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `Benutzername@domain.com` oder

Domain\Benutzername). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (Benutzername@domain.com und Domain\Benutzername).

2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.



Beachten Sie
Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

3.5.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche ⊗ **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile. Das ausgewählte Konto wird gelöscht.

4. INTEGRATIONEN

Managed-Service-Anbieter mit einem Partnerkonto im GravityZone Control Center können Control Center mit Drittanbieter-Lösungen integrieren, so zum Beispiel mit Lösungen für die Fernüberwachung und -verwaltung.

Die Integration Ihrer Drittanbieter-Lösungen können Sie auf der Seite **Integrationen** konfigurieren. Sie gelangen zu dieser Seite, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren und dann **Integrationen** wählen.

4.1. Integration mit ConnectWise

In Control Center ist speziell für Partner mit ConnectWise-Konten eine Integrationsfunktion verfügbar, mit der die Bitdefender-Sicherheitsdienste, die Kundenunternehmen über eine ConnectWise-Plattform zur Verfügung gestellt werden, dank automatischer Verfahren zur Ticket- und Rechnungserstellung effizient überwacht werden können.

Eine vollständige Anleitung zur Integration von GravityZone Control Center und ConnectWise finden Sie im ConnectWise-Integrationshandbuch.

4.2. Integrationen aufheben

1.
2. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle. Bestätigen Sie den Vorgang, um die ausgewählte Integration aus Control Center zu entfernen.



Wichtig

Wenn Sie eine Integration löschen, laufen alle auf der entsprechenden Plattform installierten Clients automatisch ab (d. h. sie kommunizieren nicht mehr mit Bitdefender Cloud Services oder dem Control Center und werden aus dem Control Center entfernt.

5. HILFE ERHALTEN

5.1. Verwenden des Support-Tools

Das Support-Tool von GravityZone ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Lösung von Problemen benötigen. Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Fehlersuche an einen Bitdefender-Support-Mitarbeiter.

5.1.1. Das Support-Tool unter Windows verwenden

1. Laden Sie das Support-Tool herunter und bringen Sie sie auf die betroffenen Computer aus. Um das Support-Tool herunterzuladen:
   a. Bauen Sie über Ihr Konto eine Verbindung mit der Control Center auf.
   b. Klicken Sie in der unteren linken Bildschirmecke der Konsole auf **Hilfe und Support**.
   c. Die Download-Links finden Sie im **Support**-Bereich. Es stehen zwei Versionen zur Verfügung: eine für 32-Bit-Systeme und eine für 64-Bit-Systeme. Stellen Sie sicher, dass Sie die richtige Version verwenden, wenn Sie das Support-Tool auf einem Computer ausführen.
2. Führen Sie das Support-Tool lokal auf jedem der betroffenen Computer aus.
   a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.
   b. Geben Sie in das Formular die nötigen Daten ein:
      i. Geben Sie Ihre E-Mail-Adresse ein.
      ii. Geben Sie Ihren Namen ein.
      iii. Wählen Sie Ihr Land aus dem entsprechenden Menü.
      iv. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.
      v. Sie können auch versuchen das Problem zu reproduzieren, bevor Sie mit der Datensammlung beginnen. Gehen Sie in diesem Fall folgendermaßen vor:
         A. Aktivieren Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**.

B. Klicken Sie auf **Weiter**.
C. Wählen Sie die Art des aufgetretenen Problems.
D. Klicken Sie auf **Weiter**.
E. Reproduzieren Sie das Problem auf Ihrem Computer. Kehren Sie danach zum Support-Tool zurück und wählen Sie die Option **Ich habe das Problem reproduziert**.

c. Klicken Sie auf **Weiter**. Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.

d. Warten Sie, bis der Vorgang beendet ist.

e. Klicken Sie auf **Beenden**, um das Fenster zu schließen. Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt.

   Schicken Sie das ZIP-Archiv gemeinsam mit Ihrer Anfrage an einen Bitdefender-Support-Mitarbeiter. Verwenden Sie dafür das E-Mail-Support-Ticket-Formular auf der **Hilfe und Support**-Seite der Konsole.

5.1.2. Das Support-Tool unter Linux

Für Linux-Betriebssysteme ist das Support-Tool im Bitdefender-Sicherheitsagenten integriert.

Linux-Systeminformationen können Sie über das Support-Tool mit dem folgendem Befehl erhalten:

```
# /opt/BitDefender/bin/bdconfigure
```

Dabei stehen folgende Optionen zur Verfügung:

- `--help` zeigt eine Liste aller Support-Tool-Befehle an.
- `enablelogs` aktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `disablelogs` deaktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `deliverall` erstellt ein Archiv, das die Produkt- und Kommunikationsmodulprotokolle enthält. Es wird an den Ordner `/tmp` im

folgenden Format zugestellt: `bitdefender_Maschinenname_Zeitstempel.tar.gz`.

1. Wenn Sie die Protokolle deaktivieren möchten, werden Sie um eine Bestätigung gebeten. Wenn nötig, werden die Dienste automatisch neu gestartet.
2. Wenn Sie Protokolle löschen möchten, werden Sie um eine Bestätigung gebeten.

- `deliverall -default` lLiefert dieselben Informationen wie die vorige Option, aber Standardaktionen werden auf die Protokolle ausgeführt, ohne dass der Benutzer dies bestätigt (die Protokolle werden deaktiviert und gelöscht).

So melden Sie ein GravityZone-Problem, das Ihre Linux-Systeme beeinträchtigt (verwenden Sie dazu die oben beschriebenen Optionen):

1. Aktivieren Sie Produkt- und Kommunikationsmodulprotokolle.
2. Versuchen Sie, das Problem nachzustellen.
3. Deaktivieren Sie Protokolle.
4. Erstellen Sie ein Protokollarchiv.
5. Öffnen Sie ein E-Mail-Support-Ticket über das Formular auf der Seite **Hilfe & Support** des Control Center; geben Sie eine Beschreibung des Problems ein und hängen Sie das Protokollarchiv an.

Das Support-Tool für Linux liefert die folgenden Informationen:

- Die Ordner `etc`, `var/log`, `/var/crash` (sofern vorhanden) und `var/epag` von `/opt/BitDefender`; darin sind die Bitdefender-Protokolle und -Einstellungen enthalten.
- Die Datei `/tmp/bdinstall.log`, die Installationsinformationen enthält.
- Die Datei `network.txt`, die Netzwerkeinstellungen und Informationen zur Netzwerkverbindung der Maschine enthält.
- Die Datei `system.txt`, die allgemeine Systeminformationen enthält (Distribution und Kernel-Version, verfügbarer RAM und freier Festplattenspeicher)
- Die Datei `users.txt`, die Benutzerinformationen enthält
- Andere Informationen zum Produkt im Zusammenhang mit dem Systen, z. B. externe Verbindungen von Prozessen und CPU-Auslastung

- Systemprotokolle